Available online at www.sciencedirect.com
SCIENCE DIRECT
Journal of Algebra 284 (2005) 669–678
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

On Thompson's finiteness theorem

Mong Lung Lang

Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore

Received 14 April 2004
Available online 13 December 2004
Communicated by Gordon James

Abstract

In this article, we give an alternative (constructive) proof of Thompson's finiteness theorem.

Keywords: Congruence subgroups; Modular group

1. Introduction

The finiteness of the collection of all congruence subgroups of $PSL_2(\mathbb{Z})$ of genus zero was first conjectured by H. Rademacher. This follows immediately by a much more general result of J. Thompson [9]: Let Γ be a subgroup of $PSL_2(\mathbb{R})$ that is commensurable with $PSL_2(\mathbb{Z})$. Denote by $g(\Gamma)$ its genus and by $\chi(\Gamma)$ its Euler characteristic,

$$\chi(\Gamma) = 2\big(g(\Gamma) - 1\big) + c + \sum_{i=1}^{r} \big(1 - e_i^{-1}\big),$$

where c is the number of cusps of Γ, r is the number of non-conjugate elliptic subgroups of Γ, and $e_1, \dots, e_r$ are their orders. Let $\mathcal{K}$ be the set of all congruence subgroups of Γ.

E-mail address: matlml@math.nus.edu.sg.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2004.10.019

Then

$$\lim_{K\in\mathcal{K}} \frac{g(K)}{[\Gamma : K]} = \frac{1}{2}\chi(\Gamma),$$

in the sense that for any $\epsilon > 0$, there are only finitely many elements K of $\mathcal{K}$ such that

$$\left|\frac{g(K)}{[\Gamma : K]} - \frac{1}{2}\chi(\Gamma)\right| > \epsilon.$$

As the above does not tell anything about the index $[\Gamma : K]$, it is P. Zograf, in his article [10], gives a lower bound for the genus of K in terms of its index in Γ and the Euler characteristic of Γ. Suggested by this work of Zograf [10] and works of Conway [1], we shall give an alternative proof of the following result of Thompson:

For each integer g, there are only finitely many discrete subgroups K of $PSL_2(\mathbb{R})$ such that:
(a) $\Gamma_0(N) \subseteq K$ *for some* N, $g(K) \leqslant g$,
(b) $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ *generates the stabiliser of the infinite cusp.*

In particular, we shall prove, in Section 5, that if K is a group as mentioned above, then

$$K \subseteq M = \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix}^{-1} \Gamma_0^+(f) \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix},$$

where

(i) f is square-free, $1 + g > 3\chi(\Gamma_0^+(f))/64$;
(ii) $x \in \mathbb{N}$, $(y, h) = 1$, $0 \leqslant y < h$, $h \mid 24$, $64(g+1)/3\chi(\Gamma_0^+(f)) > x$;
(iii) level of $K < 64(g+1)[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap M]/3\chi(\Gamma_0^+(f))$.

Recall that level of K is the smallest $N \in \mathbb{N}$ such that $\Gamma(N) \subseteq K$, $\chi(\Gamma_0^+(f)) = 6^{-1}\prod_{p|n}(p+1)/2$, and $\Gamma(N)$, $\Gamma_0(N)$, $\Gamma_0^+(N)$ are defined as follows:

(a) $\Gamma_0(N) = \left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\colon c \equiv 0 \pmod N\right\}$, $\Gamma(N) = \{A\colon A \equiv \pm I \pmod N\}$.
(b) Let e be an exact divisor of N ($\gcd(e, N/e) = 1$). An Atkin–Lehner involution w_e associated to $\Gamma_0(N)$ is a matrix of determinant 1 of the form

$$w_e = \begin{pmatrix} a\sqrt{e} & b/\sqrt{e} \\ cN/\sqrt{e} & d\sqrt{e} \end{pmatrix}, \quad \text{where } a, b, c, d, N \in \mathbb{Z}.$$

$\Gamma_0^+(N)$ is the group generated by $\Gamma_0(N)$ and all the Atkin–Lehner involutions associated to $\Gamma_0(N)$.

By (i) and (ii), if g is fixed, then the choices of x, y, h, and f are finite. In particular, the number of choices of M is finite. For each M satisfying (i)–(iii), the level of K is bounded by $64(g+1)[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap M]/3\chi(\Gamma_0^+(f))$. In particular, the number of choices of K in M is finite. As a consequence, the number of choices of K satisfying (a) and (b) is finite. Note that $[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap M]$ has been determined (see Section 2.3). The slight difference between Thompson's original proof and ours is that Thompson's proof does not provide an upper bound for the level of K while ours does. In the case $g = 0$, such groups have relevance to the Monster simple group [3,4,9]. The main facts used in our proof are results of M.L. Lang (see Section 2.3) and the following:

(C) (J.H. Conway [1]) Let G be a subgroup of $PSL_2(\mathbb{Z})$ of finite index. Then M is a maximal discrete supergroup of G if and only if M is the setwise stabiliser of a cell $c(f, \sigma) \subseteq \Omega(G)$.

(Z) (P. Zograf [10]) Let Γ be a subgroup of $PSL_2(\mathbb{R})$ commensurable with $PSL_2(\mathbb{Z})$ and let G be a congruence subgroup of Γ. Then $g(G) + 1 > 3\chi(\Gamma)[\Gamma : G]/64$.

More details about (C) and (Z) can be found in Section 2. As a byproduct of our study, the following result can be found in Appendix A.

Theorem A.4. *For each integer $g \geqslant 0$, the number of conjugacy classes of discrete congruence subgroups of $PSL_2(\mathbb{R})$ of genus at most g is finite. Every conjugacy class $Cl(G)$ admits a representative X in $\Gamma_0^+(f)$ for some f, where*

(i) *f is square-free, $1 + g \geqslant 1 + g(\Gamma_0^+(f)) > 3\chi(\Gamma_0^+(f))/64 = \frac{1}{128}\prod_{p|f}(p+1)/2$;*

(ii) *X is a congruence of level r, where r is a divisor of n^2 (level of G is n) and $64(g+1) \times [PSL_2(\mathbb{Z}) : \Gamma_0(f)]/3\chi(\Gamma_0^+(f)) > r$.*

It is our duty to point out that the proofs of the Thompson's finiteness theorem, (C), and (Z) are nontrivial and that our constructive proof of Thompson's finiteness theorem is just an elementary application of (C), (Z), and Lang [6]. It is also worthwhile to point out that congruence subgroups of $\Gamma_0^+(n)$ of genus 0 and 1 has been determined by C.J. Cummins [2].

2. Known results

2.1. Results of Helling, Larcher, Stothers, and Zograf

Results of Larcher and Zograf give bounds of the levels and indices of a congruence subgroups of $PSL_2(\mathbb{R})$.

Theorem (P. Zograf [10]). *Let Γ be a subgroup of $PSL_2(\mathbb{R})$ commensurable with $PSL_2(\mathbb{Z})$ and let G be a congruence subgroup of Γ. Then $g(G) + 1 > 3\chi(\Gamma)[\Gamma : G]/64$, where*

$\chi(\Gamma)$ is the Euler characteristic,

$$\chi(\Gamma) = 2\bigl(g(\Gamma) - 1\bigr) + c + \sum_{i=1}^{r}(1 - 1/e_i),$$

c is the number of cusps of Γ, r is the number of conjugacy classes of elliptic subgroups of Γ, and $e_1, e_2, \ldots, e_r$ are their orders.

Remark. (i) Let $n \in \mathbb{N}$. Then $\chi(\Gamma_0^+(n)) = \frac{n}{6}\prod_{p|n}(p+1)/2p$.

(ii) Suppose that $g \geqslant g(\Gamma_0^+(f))$. By Zograf's theorem ($\Gamma = G = \Gamma_0^+(f)$), $1 + g \geqslant 1 + g(\Gamma_0^+(f)) > 3\chi(\Gamma_0^+(f))/64$.

Theorem (H. Helling [5]). *Let G be a subgroup of $PSL_2(\mathbb{R})$ commensurable with $PSL_2(\mathbb{Z})$. Then G is a subgroup of $\sigma^{-1}\Gamma_0^+(f)\sigma$, where σ is a matrix with rational entries and f is square-free.*

Theorem (H. Larcher [7], W.W. Stothers [8]). *Suppose that G is a congruence of level m. Then $[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap G] \geqslant m$.*

2.2. Results of Conway: lattices commensurable with $\mathbb{Z} \times \mathbb{Z}$

The material of this section is taken from *Understanding groups like $\Gamma_0(N)$*. The readers are referred to [1] for more detail.

Denote the set of all lattices commensurable with $\mathbb{Z} \times \mathbb{Z}$ by Ψ (two lattices X and Y are commensurable with each other if $X \cap Y$ is of finite indices in both X and Y). Two lattices X and Y in Ψ are equivalent to each other if there exists some $\lambda \in \mathbb{Q}^\times$ such that $\lambda X = Y$. It is clear that the above relation is an equivalence relation defined on Ψ and each equivalence class has a unique representative of the form $L(M, g/h) = \langle (M, g/h), (0, 1)\rangle$, where $M \in \mathbb{Q}^+$, $h \in \mathbb{N}$, and $0 \leqslant g/h < 1$ is a fraction in its least terms. The equivalence class that contains $L(M, g/h)$ is denoted by $\Lambda(M, g/h)$. The set of all classes is denoted by Ω.

Definition. Let $f \in \mathbb{N}$ be square-free and let σ be a nonsingular matrix with rational entries. The $c(f, \sigma)$ cell associated to f and σ is the set $\{\Lambda(m, 0)\sigma\colon\ m \mid f\}$.

Theorem 2.1. *The setwise stabiliser of the $c(f, \sigma)$ cell is $\sigma^{-1}\Gamma_0^+(f)\sigma$.*

Definition. Let G be a subgroup of $PSL_2(\mathbb{Z})$. The set of all classes invariant under G is denoted by $\Omega(G)$.

Theorem 2.2. *A class $\Lambda(M, g/h)$ is invariant under $\Gamma_0(n)$ if and only if $M \in \mathbb{N}$ and M is a divisor of n/h^2, where h is a divisor of 24.*

Theorem 2.3. *Let G be a subgroup of $PSL_2(\mathbb{Z})$ of finite index. Then $M \subseteq PSL_2(\mathbb{R})$ is a maximal discrete supergroup of G if and only if M is the setwise stabiliser of a cell $c(f,\sigma) \subseteq \Omega(G)$.*

2.3. Results of Lang on $[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap M]$

In [6], the author studies the index $[M : M \cap N]$, where M and N are maximal discrete subgroups of $PSL_2(\mathbb{R})$ that are commensurable with $PSL_2(\mathbb{Z})$. In particular, let

$$M = \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix}^{-1} \Gamma_0^+(f) \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix},$$

where f is square-free, $x \in \mathbb{Q}^+$, $0 \leqslant y < h$, $\gcd(y,h) = 1$. For each divisor d of f, define

(i) $dx = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, $dy/h = d_0/p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$, where $p_1, p_2, \ldots, p_r$ are primes, $\gcd(d_0, p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}) = 1$, $a_i \in \mathbb{Z}$, $b_i \in \mathbb{N} \cup \{0\}$,
(ii) $m_d = \prod p_i^{b_i + |a_i + b_i|}$.

Then the index $[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap M]$ is given by $[PSL_2(\mathbb{Z}) : \Gamma_0(mf)]$, where $m = \min\{m_d \colon d \mid f\}$.

3. Supergroups of $\Gamma_0(n)$

Proposition 3.1. *$M \leqslant PSL_2(\mathbb{R})$ is a maximal discrete supergroup of $\Gamma_0(n)$ if and only if*

$$M = \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix}^{-1} \Gamma_0^+(f) \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix},$$

where f is square-free, $\gcd(y,h) = 1$, $h \mid 24$, $0 \leqslant y < h$, $x \in \mathbb{N}$, $xh^2 \mid n$, and $xfh^2 \mid n(f,h)^2$.

Proof. Let $M \leqslant PSL_2(\mathbb{R})$ be a maximal discrete supergroup of $\Gamma_0(n)$. It follows that M is commensurable with $PSL_2(\mathbb{Z})$. By Helling's theorem, M takes the following form: $M = \nu^{-1}\Gamma_0^+(f)\nu$, where f is square-free and ν is a matrix with rational entries. Suppose that $\nu(\infty) = r$. Since ∞ is the only cusp of $\Gamma_0^+(f)$, there exists $\tau \in \Gamma_0^+(f)$ such that $\tau(r) = \infty$. This implies that $\tau\nu(\infty) = \infty$. Hence $\tau\nu = \left(\begin{smallmatrix} u & v \\ 0 & w \end{smallmatrix}\right)$. This implies that

$$M = \begin{pmatrix} u & v \\ 0 & w \end{pmatrix}^{-1} \Gamma_0^+(f) \begin{pmatrix} u & v \\ 0 & w \end{pmatrix}.$$

Since

$$A = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$$

normalises $\Gamma_0^+(f)$, we may replace $\Gamma_0^+(f)$ by $g^{-1}\Gamma_0^+(f)g$ ($g \in A$) if necessary. As a consequence, M takes the following form:

$$M = \begin{pmatrix} u & v \\ 0 & w \end{pmatrix}^{-1} \Gamma_0^+(f) \begin{pmatrix} u & v \\ 0 & w \end{pmatrix} = \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix}^{-1} \Gamma_0^+(f) \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix},$$

where $x \in \mathbb{Q}^+$, $\gcd(y, h) = 1$, $0 \leqslant y < h$. By Theorem 2.1, M is the setwise stabiliser of $c(f, \sigma)$, where

$$\sigma = \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix}.$$

By Theorem 2.3, $c(f, \sigma)$ is a cell of $\Omega(\Gamma_0(n))$. This implies that every class in $c(f, \sigma)$ is fixed by $\Gamma_0(n)$. Note that $c(f, \sigma) = \{\Lambda(dx, dy/h)\colon d \mid f\}$. By Theorem 2.2, h is a divisor of 24, $dx \in \mathbb{N}$, and $xdh^2 \mid n(d, h)^2$. Since f is square-free, the above is equivalent to $x \in \mathbb{N}$, $xh^2 \mid n$, and $xfh^2 \mid n(f, h)^2$. Conversely, let M be given as in the lemma. It is clear that M is the setwise stabiliser of $c(f, \sigma)$, where

$$\sigma = \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix}.$$

By Theorem 2.2, $c(f, \sigma)$ is fixed by $\Gamma_0(n)$. By Theorem 2.3, M is a maximal discrete supergroup of $\Gamma_0(n)$. □

Corollary 3.2. *Let $n \in \mathbb{N}$. The number of discrete subgroups of $PSL_2(\mathbb{R})$ that contains $\Gamma_0(n)$ is finite.*

Proof. Let K be a discrete subgroup of $PSL_2(\mathbb{R})$ that contains $\Gamma_0(n)$. By Proposition 3.1, $\Gamma_0(n) \subseteq K \subseteq M$, where M is given as in Proposition 3.1. Since $[M : \Gamma_0(n)]$ and the choices of such M are both finite, the number of discrete subgroups of $PSL_2(\mathbb{R})$ that contains $\Gamma_0(n)$ is finite. □

4. Congruence subgroups of *M*

Lemma 4.1. *Let M be a maximal discrete subgroup of $PSL_2(\mathbb{R})$ commensurable with $PSL_2(\mathbb{Z})$ and let G be a congruence subgroup of M of level r. Then*

$$[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap M][M : G] \geqslant r.$$

Proof. Applying Larcher and Stothers' theorem, $[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap G] \geqslant r$. Hence

$$\begin{aligned} &[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap M][M : G] \\ &\quad \geqslant [PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap M][PSL_2(\mathbb{Z}) \cap M : PSL_2(\mathbb{Z}) \cap G] \\ &\quad = [PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap G] \geqslant r. \qquad \square \end{aligned}$$

Lemma 4.2. *Let $G \leqslant M = \sigma^{-1}\Gamma_0^+(f)\sigma$, where f is square-free. Suppose that $g(G) \leqslant g$ and that G is a congruence of level r. Then*

$$u_M = 64(g+1)[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap M]/3\chi\big(\Gamma_0^+(f)\big) > r.$$

Proof. Applying Zograf's theorem, Lemma 4.1, and the fact that $\chi(M) = \chi(\Gamma_0^+(f))$, we have $64(g(G)+1)[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap M]/3\chi(\Gamma_0^+(f)) > r$. This completes the proof of the lemma. $\square$

Remark. $[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap M]$ can be found in Section 2.3.

Proposition 4.3. *Let M be a maximal subgroup of $PSL_2(\mathbb{R})$ that commensurable with $PSL_2(\mathbb{Z})$. The number of congruence subgroups of M of genus $\leqslant g$ is finite.*

Proof. By Helling's theorem, M is a conjugate of $\Gamma_0^+(f)$. Let K be a congruence subgroup of M of genus $\leqslant g$. By Lemma 4.2, the level of K is at most $u_M = 64(g+1) \times [PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap M]/3\chi(\Gamma_0^+(f))$. Since the number of congruence subgroups of M of level $\leqslant u_M$ is finite, M possesses only finitely many congruence subgroups of genus at most g. $\square$

5. Finiteness theorem of Thompson

Finiteness theorem of Thompson. *For each integer g, there are only finitely many discrete subgroups K such that*:

(a) *$\Gamma_0(N) \subseteq K$ for some N, $g(K) \leqslant g$,*
(b) *$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ generates the stabiliser of the infinite cusp.*

Further, let K be a group mentioned above, then

$$K \subseteq M = \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix}^{-1} \Gamma_0^+(f) \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix},$$

where

(i) *f is square-free, $1 + g > 3\chi(\Gamma_0^+(f))/64$;*
(ii) *$x \in \mathbb{N}$, $(y,h) = 1$, $0 \leqslant y < h$, $h \mid 24$, $64(g+1)/3\chi(\Gamma_0^+(f)) > x$;*
(iii) *level of $K < 64(g+1)[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap M]/3\chi(\Gamma_0^+(f))$.*

Proof. By Proposition 3.1,

$$K \subseteq M = \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix}^{-1} \Gamma_0^+(f) \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix},$$

where f is square-free, $x \in \mathbb{N}$, $0 \leqslant y < h$, $\gcd(y,h) = 1$, h is a divisor of 24. Since $g(M) \leqslant g(K) \leqslant g$, by Zograf's theorem,

$$1 + g \geqslant 1 + g(K) \geqslant 1 + g(M) > 3\chi(M)/64 = 3\chi\big(\Gamma_0^+(f)\big)/64.$$

Since

$$M_\infty = \left\langle \begin{pmatrix} 1 & 1/x \\ 0 & 1 \end{pmatrix} \right\rangle, \qquad K_\infty = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle,$$

by Zograf's theorem, we have

$$64(g+1)/3\chi\big(\Gamma_0^+(f)\big) > [M : K] \geqslant [M_\infty : K_\infty] \geqslant x.$$

By Lemma 4.2, level of K is at most $64(g+1)[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap M]/3\chi(\Gamma_0^+(f))$ (see Section 2.3 for $[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap M]$). In summary, we have

(i) f is square-free, $1 + g > 3\chi(\Gamma_0^+(f))/64$;
(ii) $x \in \mathbb{N}$, $(y,h) = 1$, $0 \leqslant y < h$, $h \mid 24$, $64(g+1)/3\chi(\Gamma_0^+(f)) > x$;
(iii) level of $K < 64(g+1)[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap M]/3\chi(\Gamma_0^+(f))$.

By (i) and (ii), the number of choices of M is finite. For each M satisfies (i) and (ii), the number of choices of $K \subseteq M$ is finite. As a consequence, the number of choices of K that satisfies (a) and (b) of the theorem is finite. □

Appendix A

In this appendix, we prove, in Theorem A.4, that there are only finitely many conjugacy classes of discrete congruence subgroups of $PSL_2(\mathbb{R})$ of genus at most g.

Lemma A.1. *$M \subseteq PSL_2(\mathbb{R})$ is a maximal discrete supergroup of $\Gamma(n)$ if and only if*

$$M = \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix}^{-1} \Gamma_0^+(f) \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix},$$

where f is square-free, $xn \in \mathbb{N}$, $\gcd(y,h) = 1$, $0 \leqslant y < h$, $xnh^2 \mid n^2$, and $xfnh^2 \mid n^2(f,h)^2$.

Proof. By Lemma A1 of [6], a class $\Lambda(x, y/h)$ ($\gcd(y,h) = 1$) is invariant under $\Gamma(n)$ if and only if $xn \in \mathbb{N}$, xnh^2 is a divisor of n^2. Applying the proof of Proposition 3.1, $M \subseteq PSL_2(\mathbb{R})$ is a maximal discrete supergroup of $\Gamma(n)$ if and only if

$$M = \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix}^{-1} \Gamma_0^+(f) \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix},$$

where f is square-free, $xn \in \mathbb{N}$, $\gcd(y,h) = 1$, $0 \leqslant y < h$, $xnh^2 \mid n^2$, and $xfnh^2 \mid n^2(f,h)^2$. $\square$

Corollary A.2. *Let $n \in \mathbb{N}$. The number of discrete subgroups of $PSL_2(\mathbb{R})$ of level n is finite.*

Proof. Let K be a discrete subgroup of $PSL_2(\mathbb{R})$ of level n. By Lemma A.1, $\Gamma(n) \subseteq K \subseteq M$, where M is given as in Lemma A.1. Since $[M : \Gamma(n)]$ and the choices of such M are both finite, the number of discrete subgroups of $PSL_2(\mathbb{R})$ of level n is finite. $\square$

Lemma A.3. *Let $G \subseteq PSL_2(\mathbb{R})$ be a discrete congruence group of level n. Then there exists some σ (a matrix with rational entries), $f \in \mathbb{N}$, such that $\Gamma(n^2) \subseteq \sigma G \sigma^{-1} \subseteq \Gamma_0^+(f)$.*

Proof. Since G is discrete and $\Gamma(n) \subseteq G$, by Lemma A.1,

$$\Gamma(n) \subseteq G \subseteq \sigma^{-1}\Gamma_0^+(f)\sigma = \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix}^{-1} \Gamma_0^+(f) \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix},$$

where f is square-free, $\gcd(y,h) = 1$, $0 \leqslant y < h$, $xn \in \mathbb{N}$, $xnh^2 \mid n^2$, and $xnfh^2 \mid n^2(f,h)^2$. Let

$$\sigma = \begin{pmatrix} x & y/h \\ 0 & 1 \end{pmatrix}, \qquad A = \begin{pmatrix} \pm 1 + an^2 & bn^2 \\ cn^2 & \pm 1 + dn^2 \end{pmatrix} \in \Gamma\bigl(n^2\bigr).$$

Direct calculation shows that $\sigma^{-1}A\sigma \subseteq \Gamma(n) \subseteq G$. Hence $\Gamma(n^2) \subseteq \sigma G \sigma^{-1}$. This completes the proof of the lemma. $\square$

Theorem A.4. *For each integer $g \geqslant 0$, the number of conjugacy classes of discrete congruence subgroups of $PSL_2(\mathbb{R})$ of genus at most g is finite. Every conjugacy class $Cl(G)$ admits a representative X in $\Gamma_0^+(f)$ for some f, where*

(i) *f is square-free, $1 + g \geqslant 1 + g(\Gamma_0^+(f)) > 3\chi(\Gamma_0^+(f))/64 = \frac{1}{128}\prod_{p\mid f}(p+1)/2$;*
(ii) *X is a congruence of level r, where r is a divisor of n^2 (level of $G = n$) and $64(g+1) \times [PSL_2(\mathbb{Z}) : \Gamma_0(f)]/3\chi(\Gamma_0^+(f)) > r$.*

Proof. Let $K \subseteq PSL_2(\mathbb{R})$ be a discrete congruence group of level n, genus at most g. By Lemma A.3, $\Gamma(n^2) \subseteq \sigma K \sigma^{-1} \subseteq \Gamma_0^+(f)$ for some $f \in \mathbb{N}$, $\sigma \in PGL_2(\mathbb{Q})$. By the remark following Zograf's theorem made in Section 2.1, f satisfies (i). Let $X = \sigma K \sigma^{-1} \in Cl(K)$. Since $\Gamma(n^2) \subseteq X \subseteq \Gamma_0^+(f)$, X is a congruence of level r, where r is a divisor of n^2. By Lemma 4.2 ($M = \Gamma_0^+(f)$, $G = X$), $64(g+1)[PSL_2(\mathbb{Z}) : \Gamma_0(f)]/3\chi(\Gamma_0^+(f)) \geqslant r$. It is clear that if g is fixed, then the choices of f and r are finite. As a consequence, the number of choices of X is finite. Hence the number of choices of $Cl(K)$ is finite. This completes the proof of our theorem. $\square$

References

[1] J.H. Conway, Understanding groups like $\Gamma_0(N)$, in: Groups, Difference Sets and the Monster, Columbus, OH, 1993, in: Ohio State Univ. Math. Res. Inst. Publ., vol. 4, de Gruyter, Berlin, 1996, pp. 327–343.

[2] C.J. Cummins, Congruence subgroups of groups commensurable with $PSL(2, \mathbb{Z})$ of genus 0 and 1, preprint.

[3] C.J. Cummins, T. Gannon, Modular equations and the genus zero property of moonshine functions, Invent. Math. 129 (1997) 413–443.

[4] J.H. Conway, S.P. Norton, Monstrous moonshine, Bull. London Math. Soc. 11 (1979) 308–338.

[5] H. Helling, Bestimmung der Kommensurabilitätsklasse der Hilbertschen Moulgruppe, Math. Z. 92 (1966) 269–280.

[6] M.L. Lang, Groups commensurable with the modular group, J. Algebra 274 (2) (2004) 804–822.

[7] H. Larcher, The cusp amplitudes of the congruence subgroups of the classical modular group, Illinois J. Math. 26 (1) (1982) 164–172.

[8] W.W. Stothers, Level and index in the modular group, Proc. Roy. Soc. Edinburgh Sect. A 99 (1984) 115–126.

[9] J.G. Thompson, A finiteness theorem for subgroups of $PSL_2(\mathbb{R})$ which are commensurable with $PSL_2(\mathbb{Z})$, in: Proc. Sympos. Pure Math., vol. 37, Amer. Math. Soc., 1980, pp. 533–555.

[10] P. Zograf, A spectral proof of Rademacher's conjecture for congruence subgroups of the modular group, J. Reine Angew. Math. 414 (1991) 113–116.